AMENDMENTS TO THE CLAIMS

Claim 1 (Currently Amended) A key issuing server apparatus ~~prime calculating apparatus~~ for calculating a prime candidate N larger than a known prime q and testing primality of the calculated prime candidate N and for issuing a public key and a private key of an RSA encryption system for a terminal, the key issuing server apparatus comprising:

an information storage unit storing the known prime q, management information that is an odd number and corresponds to a prime to be generated, and a predetermined verification value;

a random number generation unit operable to generate a random number;

a candidate calculation unit operable to (i) read the prime q, the management information, and the verification value, (ii) calculate a multiplication value R by multiplying the management information by the random number, and (iii) calculate the prime candidate N, according to $N = 2 \times$ (the multiplication value $R + w$) $\times$ the prime $q + 1$, using w satisfying $2 \times w \times$ the prime $q + 1 =$ the verification value (*mod* the management information);

a primality testing unit operable to test primality of the calculated prime candidate N; ~~and~~

an output unit operable to output the calculated prime candidate N as a prime N when the primality of the calculated prime candidate N is determined; and

a key output unit operable to output the private key and the public key of the RSA encryption system to the terminal, the private key and the public key being generated using the prime N output by the output unit.

Claim 2 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 1, ~~wherein~~

wherein the verification value stored in the information storage unit is 1, and

wherein the candidate calculation unit calculates the prime candidate N according to $N = 2 \times$ the multiplication value $R \times$ the prime $q + 1$.

Claim 3 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 1, wherein the primality testing unit includes:

a 1st judging subunit operable to judge whether the prime candidate N satisfies $2^{N-1} = 1 \ mod \ N$; and

a 2nd judging subunit operable to perform, when the judgment of the 1st judging subunit is affirmative, one of ~~judgments of~~ (i) a judgment of whether the prime candidate N and the multiplication value R satisfy $2^{2R} \neq 1 \ mod \ N$ and (ii) a judgment of whether the prime candidate N and the multiplication value R satisfy $GCD(2^{2R}-1, N) = 1$, and to determine the primality of the prime candidate N when the judgment performed by the 2nd judging subunit ~~one of judgments~~ is affirmative.

Claim 4 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 1, ~~wherein~~

wherein the information storage unit further stores a known prime g and a unique issue identifier, and

wherein the key issuing server ~~prime calculating~~ apparatus further comprises ~~comprising~~:

a prime generation unit operable to generate a prime *gp* by applying a prime generation function for generating a unique prime to the prime *g* and the unique issue identifier, and output the generated prime *gp*; and

a writing unit operable to write the generated prime *gp* to the information storage unit as the management information.

Claim 5 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 4, wherein the prime generation unit (i) generates a combination of the unique issue identifier and a variable *c* that is one of 0 and a positive integer, (ii) calculates a prime candidate = 2 × the prime $g \times f$(the combination) + 1, and (iii) tests primality of the calculated prime candidate, and outputs the calculated prime candidate as the prime *gp* when the primality of the calculated prime candidate is determined.

Claim 6 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 5, wherein, when the primality of the calculated prime candidate is not determined, the prime generation unit (i) adds a value of 1 to the variable *c*, (ii) generates a 2nd combination of the unique issue identifier and the variable *c* having the value of 1 added thereto, (iii) calculates a 2nd prime candidate = 2 × the prime $g \times f$(the 2nd combination) + 1, and (iv) tests primality of the 2nd calculated prime candidate, and outputs the 2nd calculated prime

candidate as the prime *gp* when the primality of the 2nd calculated prime candidate is determined.

Claim 7 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 1, further comprising[[:]] an iteration control unit operable to control the random number generation unit, the candidate calculation unit, and the primality testing unit to iterate the generation of the random number ~~generation~~, the calculation of the prime candidate N, and the primality testing, until the primality of the calculated prime candidate N is determined by the primality testing unit.

Claim 8 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 7, further comprising:

a preparative prime storage unit storing a known prime p;

a preparative random number calculation unit operable to calculate a random number R';

a preparative candidate calculation unit operable to calculate a prime candidate N', according to $N' = 2 \times$ the random number $R' \times$ the prime $p + 1$, using the prime p and the calculated random number R';

a preparative primality testing unit operable to test primality of the calculated prime candidate N';

a preparative writing unit operable to write the calculated prime candidate N' to the information storage unit as [[a]] the prime q when the primality of the calculated prime candidate

N' is determined; and

a preparative iteration control unit operable to control the preparative random number calculation unit, the preparative candidate calculation unit, and the preparative primality testing unit to iterate the calculation of the random number R', the calculation of the prime candidate N', and the primality testing, until the primality of the calculated prime candidate N' is determined by the preparative primality testing unit.

Claim 9 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 7 further comprising ~~that is~~ a key generating apparatus for generating [[a]] the public key and [[a]] the private key of the RSA encryption system, the key generating apparatus including ~~further comprising~~:

a public key generation unit operable to generate the public key using [[a]] the ~~calculated~~ prime N output by the output unit; and

a private key generation unit operable to generate the private key using the prime N output by the output unit ~~generated public key~~.

Claim 10 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 9, ~~wherein~~

wherein the public key generation unit (i) directs the iteration control unit to newly obtain a prime N', (ii) calculates a number n, according to $n =$ the prime $N \times$ the prime N', using the prime N and the newly obtained prime N', and (iii) generates a random number e,

wherein a combination of the calculated number n and the generated random number e

is the public key,

wherein the private key generation unit calculates d satisfying $e \times d = 1 \ mod \ L$,

wherein L is a least common multiple of the prime N - 1 and the prime N' - 1, and

wherein the calculated d is the private key.

Claim 11 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 9, ~~wherein~~

wherein the information storage unit further stores a different verification value from the verification value,

wherein the public key generation unit directs the iteration control unit to newly obtain a prime N',

wherein the candidate calculation unit calculates a prime candidate N', as the prime N', according to $N' = 2 \times$ the multiplication value $R \times$ the prime $q +$ the different verification value,

wherein the public key generation unit calculates a number n, according to $n =$ the prime $N \times$ the prime N', using the prime N and the newly obtained prime N', and generates a random number e,

wherein a combination of the calculated number n and the generated random number e is the public key,

wherein the private key generation unit calculates d satisfying $e \times d = 1 \ mod \ L$,

wherein L is a least common multiple of the prime N - 1 and the prime N' - 1, and

wherein the calculated d is the private key.

Claim 12 (Cancelled)

Claim 13 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 9 ~~Claim 12~~, further comprising:

an identifier obtaining unit operable to obtain a terminal identifier uniquely identifying the terminal;

a management information generation unit operable to generate the management information including the obtained terminal identifier; and

a writing unit operable to write the generated management information to the information storage unit.

Claim 14 (Currently Amended) The key issuing server apparatus ~~prime calculating apparatus~~ of Claim 13, further comprising[[:]] a server identifier storage unit prestoring a server identifier uniquely identifying ~~the prime calculating apparatus functioning as~~ the key issuing server apparatus, ~~wherein~~

wherein the management information generation unit further reads the server identifier from the server identifier storage unit, and generates the management information further including the read server identifier.

Claim 15 (Currently Amended) A key ~~prime~~ verification server apparatus for verifying ~~the~~ a prime N output by ~~a prime calculating apparatus~~ key issuing server apparatus for calculating a prime candidate N larger than a known prime q, testing primality of the calculated prime

candidate N, and generating and issuing a public key and a private key of an RSA encryption system for a terminal, the key issuing server apparatus including an information storage unit storing the known prime q, management information that is an odd number and corresponds to a prime to be generated, and a predetermined verification value, a random number generation unit operable to generate a random number, a candidate calculation unit operable to (i) read the prime q, the management information, and the verification value, (ii) calculate a multiplication value R by multiplying the management information by the random number, and (iii) calculate the prime candidate N, according to $N = 2 \times$ (the multiplication value $R + w$) $\times$ the prime $q + 1$, using w satisfying $2 \times w \times$ the prime $q + 1$ = the verification value (*mod* the management information), a primality testing unit operable to test primality of the calculated prime candidate N, an output unit operable to output the calculated prime candidate N as the prime N when the primality of the calculated prime candidate N is determined, and a key output unit operable to output the private key and the public key of the RSA encryption system to the terminal, the private key and the public key being generated using the prime N output by the output unit ~~of Claim 1~~, the key verification server apparatus comprising:

a prime-verification-apparatus information storage unit storing the management information and the verification value;

a subtraction unit operable to obtain a prime subtraction value by subtracting the verification value from the prime N;

a judgment unit operable to judge whether the obtained prime subtraction value is divisible by the management information; and

a control unit operable to permit use of the prime N when the judgment by the judgment

unit is affirmative, and prohibit the use of the prime N when the judgment by the judgment unit is negative.

Claim 16 (Currently Amended) The key ~~prime~~ verification server apparatus of Claim 15, ~~wherein~~

wherein the key issuing server ~~prime calculating~~ apparatus stores the verification value which is 1, and calculates [[a]] the prime candidate N, according to $N = 2 \times$ the multiplication value $R \times$ the prime $q + 1$,

wherein the verification value stored in the prime-verification-apparatus information storage unit is 1, and

wherein the subtraction unit obtains the prime subtraction value by subtracting 1 from the prime N.

Claim 17 (Currently Amended) The key ~~prime~~ verification server apparatus of Claim 15, ~~wherein~~

wherein the key issuing server ~~prime calculating~~ apparatus further (i) stores a known prime g and a unique issue identifier, (ii) generates a prime gp by applying a prime generation function for generating a unique prime using the prime g and the unique issue identifier, (iii) outputs the generated prime gp, and (iv) writes the generated prime gp to the information storage unit as the management information, ~~and~~

wherein the prime-verification-apparatus information storage unit further stores the

prime g and the unique issue identifier, and

wherein the key ~~prime~~ verification server apparatus further comprises ~~comprising~~:

a prime generation unit operable to generate the prime gp by applying the prime generation function for generating the unique prime using the prime g and the unique issue identifier, and output the generated prime gp; and

a writing unit operable to write the generated prime gp to the prime-verification-apparatus information storage unit as the management information.

Claim 18 (Currently Amended) The key~~prime~~ verification server apparatus of Claim 17,

wherein the key issuing server ~~prime calculating~~ apparatus (i) generates a combination of the unique issue identifier and a variable c that is one of 0 and a positive integer, (ii) calculates a prime candidate = $2 \times$ the prime $g \times f$(the combination) + 1, (iii) tests primality of the calculated prime candidate, and (iv) outputs the calculated prime candidate as the prime gp when the primality is determined, and

wherein the prime generation unit (i) generates the combination of the unique issue identifier and the variable c, (ii) calculates the prime candidate = $2 \times$ the prime $g \times f$(the combination) + 1, and (iii) tests primality of the calculated prime candidate, and outputs the calculated prime candidate as the prime gp when the primality is determined.

Claim 19 (Currently Amended) The key ~~prime~~ verification server apparatus of Claim 18,

wherein, when the primality of the calculated prime candidate is not determined, the key issuing server ~~prime calculating~~ apparatus (i) adds a value of 1 to the variable c, (ii)

generates a 2nd combination of the unique issue identifier and the variable *c* having the value of 1 added thereto, (iii) calculates a 2nd prime candidate = 2 × the prime $g \times f$(the 2nd combination) + 1, and (iv) tests primality of the 2nd calculated prime candidate and outputs the 2nd calculated prime candidate as the prime *gp* when the primality of the 2nd calculated prime candidate is determined, and

wherein, when the primality of the ~~generated~~ calculated prime candidate is not determined, the prime generation unit (i) adds the value of 1 to the variable *c*, (ii) generates the 2nd combination of the unique issue identifier and the variable *c* having the value of 1 added thereto, and (iii) tests primality of the 2nd calculated prime candidate and outputs the 2nd calculated prime candidate as the prime *gp* when the primality of the 2nd calculated prime candidate is determined.

Claim 20 (Currently Amended) The key ~~prime~~ verification server apparatus of Claim 15, wherein the key issuing server ~~prime calculating~~ apparatus further comprises ~~is~~ a key generating apparatus for generating [[a]] the public key and [[a]] the private key of the RSA encryption system, ~~and further generates the public key of RSA encryption using the output prime *N* and generates the private key of RSA encryption using the generated public key~~, and

~~the prime verification apparatus is a key verification apparatus for verifying the public key, and~~

wherein the key ~~prime~~ verification server apparatus further comprises ~~comprising:~~

an obtaining unit operable to obtain the public key; and

~~————————~~a verifying unit operable to verify validity of the ~~obtained~~ public key obtained by the obtaining unit.

Claim 21 (Currently Amended) The key ~~prime~~ verification server apparatus of Claim 20, ~~————~~wherein the key issuing server ~~prime calculating~~ apparatus (i) newly obtains a prime N', (ii) calculates a number n, according to n = the prime $N \times$ the prime N', using the prime N and the newly obtained prime N', (iii) generates a random number e, and (iv) calculates d satisfying $e \times d = 1 \ mod \ L$, where L is a least common multiple of the prime $N - 1$ and the prime $N' - 1$, and a combination of the calculated number n and the generated random number e is the public key while the calculated d is the private key,

wherein the obtaining unit obtains the combination of the number n and the random number e as the public key, and

wherein the verifying unit includes:

a subtraction subunit operable to obtain a public-key subtraction value by subtracting a square value of the verification value from the calculated ~~obtained~~ number n;

a judgment subunit operable to judge whether the obtained prime subtraction value is divisible by the management information; and

a control subunit operable to permit output of the public key when the judgment by the judgment subunit is affirmative, and prohibit the output of the public key when the judgment by the judgment subunit is negative.

Claim 22 (Currently Amended) The key ~~prime~~ verification server apparatus of Claim 20,

wherein the key issuing server ~~prime calculating~~ apparatus further (i) stores a different verification value from the verification value, (ii) newly obtains a prime N' by calculating a prime candidate N' as the prime N', according to $N' = 2 \times$ the multiplication value $R \times$ the prime $q +$ the different verification value, (iii) calculates a number n, according to $n =$ the prime $N \times$ the prime N', using the prime N and the newly obtained prime N' and generates a random number e, and (iv) calculates d satisfying $e \times d = 1 \ mod \ L$, where L is a least common multiple of the prime $N - 1$ and the prime $N' - 1$, and a combination of the calculated number n and the generated random number e is the public key while the calculated d is the private key,

wherein the prime-verification-apparatus information storage unit stores the different verification value,

wherein the obtaining unit obtains the combination of the number n and the random number e as the public key, and

wherein the verifying unit includes:

a subtraction subunit operable to obtain a multiplication value by multiplying the verification value and the different verification value and to obtain a public key subtraction value by subtracting the multiplication value from the calculated ~~obtained~~ number n;

a judgment subunit operable to judge whether the obtained prime subtraction value is divisible by the management information; and

a control subunit operable to permit output of the public key when the judgment by the judgment subunit is affirmative, and prohibit the output of the public key when the judgment by the judgment subunit is negative.

Claim 23 (Cancelled)

Claim 24 (Currently Amended) The key-~~prime~~ verification server apparatus of Claim 20-~~Claim 23, wherein,~~

wherein the management information stored in the prime-verification-apparatus information storage unit includes a terminal identifier uniquely identifying the terminal, and

wherein the judgment unit judges whether the obtained prime subtraction value is divisible by the management information including the terminal identifier.

Claim 25 (Currently Amended) The key-~~prime~~ verification server apparatus of Claim 24, ~~wherein~~

wherein the management information stored in the prime-verification-apparatus information storage unit includes a server identifier uniquely identifying the key issuing server apparatus ~~prime calculating apparatus functioning as the key issuing server apparatus~~, and

wherein the judgment unit judges whether the obtained prime subtraction value is divisible by the management information including the server identifier.

Claim 26 (Currently Amended) The key-~~prime~~ verification server apparatus of Claim 20-~~Claim 23~~ further comprising ~~that is~~ a public-key-certificate issuing server apparatus, the public-key-certificate issuing server including ~~further comprising~~:

a certificate generation unit operable to generate, when the verifying unit determines that the public key is valid, signature data by applying a digital signature to public key

information including at least the public key, and to generate a public key certificate including at least the signature data and the public key; and

a certificate output unit operable to output the generated public key certificate.

Claim 27 (Currently Amended) A key issuing system comprising a terminal and a key issuing server apparatus for generating and issuing a private key and a public key of an RSA encryption system for the terminal, ~~wherein~~

wherein the key issuing server apparatus includes:

an information storage unit storing a known prime q, management information corresponding to a prime to be generated, and a predetermined verification value;

a random number generation unit operable to generate a random number;

a candidate calculation unit operable to (i) read the prime q, the management information, and the verification value, (ii) calculate a multiplication value R by multiplying the management information by the random number, and (iii) calculate a prime candidate N, according to $N = 2 \times$ the multiplication value $R \times$ the prime $q +$ the verification value;

a primality testing unit operable to test primality of the calculated prime candidate N;

an output unit operable to output the calculated prime candidate N as a prime N when the primality of the calculated prime candidate N is determined;

an iteration control unit operable to control the random number generation unit, the candidate calculation unit, and the primality testing unit to iterate the generation of the random number ~~generation~~, the calculation of the prime candidate N, and the primality testing,

until the primality of the calculated prime candidate N is determined by the primality testing unit;

a public key generation unit operable to generate the public key of the RSA encryption system using ~~an~~ the ~~output~~ prime N output by the output unit;

a private key generation unit operable to generate the private key of the RSA encryption system using the prime N output by the output unit ~~generated public key~~; and

a key output unit operable to output the generated private key and the public key to the terminal~~; and~~, and

~~a publishing unit operable to publish the generated public key, and~~

wherein the terminal obtains and stores the private key, and uses the stored private key.

Claim 28 (Currently Amended) The key issuing system of Claim 27, ~~wherein~~

wherein the key issuing server apparatus (i) newly obtains a prime N', (ii) calculates a number n, according to $n =$ the prime $N \times$ the prime N', using the prime N and the newly obtained prime N' and generates a random number e, and (iii) calculates d satisfying $e \times d = 1$ *mod* L, where L is a least common multiple of the prime $N - 1$ and the prime $N' - 1$, and a combination of the calculated number n and the generated random number e is the public key while the calculated d is the private key, ~~and~~

wherein the key issuing system further comprises ~~comprising~~ a key verification server apparatus ~~which includes~~ including:

an obtaining unit operable to obtain the combination of the number n and the random number e as the public key; and

a verification unit operable to verify validity of the obtained public key, and ~~wherein~~

wherein the verifying unit includes:

a subtraction subunit operable to obtain a public-key subtraction value by subtracting a square value of the verification value from the calculated ~~obtained~~ number n;

a judgment subunit operable to judge whether the obtained prime subtraction value is divisible by the management information; and

a control subunit operable to permit output of the public key when the judgment by the judgment subunit is affirmative, and prohibit the output of the public key when the judgment by the judgment subunit is negative.

Claim 29 (Currently Amended) A prime calculation method used in a key issuing server-~~prime calculating~~ apparatus that (i) includes an information storage unit storing a known prime q, management information that is an odd number and corresponds to a prime to be generated, and a predetermined verification value, and (ii) calculates a prime candidate N, as a prime N, larger than the known prime q and performs primality testing on the calculated prime candidate N, the prime calculation method comprising:

a random number generation step of generating a random number via the key issuing server apparatus;

a candidate calculation step of (i) reading the prime q, the management information, and the verification value, (ii) calculating a multiplication value R by multiplying the management information by the random number, and (iii) calculating the prime candidate N,

according to according to $N = 2 \times$ (the multiplication value $R + w$) $\times$ the prime $q + 1$, using w satisfying $2 \times w \times$ the prime $q + 1$= the verification value (*mod* the management information);

a primality testing step of testing primality of the calculated prime candidate N; ~~and~~

an output step of outputting the calculated prime candidate N as [[a]] prime N when the primality of the calculated prime candidate N is determined; and

a key output step of outputting the private key and the public key of an RSA encryption system to the terminal, the private key and the public key being generated using the prime N output by the output step.

Claim 30 (Currently Amended) A computer-readable recording medium having a prime-calculation computer program recorded thereon, the prime-calculation computer program being used on a key issuing server ~~prime calculating~~ apparatus that (i) includes an information storage unit storing a known prime q, management information that is an odd number and corresponds to a prime to be generated, and a predetermined verification value, and (ii) calculates a prime candidate N, as a prime N, larger than the known prime q and performs primality testing on the calculated prime candidate N, the prime-calculation computer program causing the key issuing server apparatus to execute a method comprising:

a random number generation step of generating a random number;

a candidate calculation step of (i) reading the prime q, the management information, and the verification value, (ii) calculating a multiplication value R by multiplying the management information by the random number, and (iii) calculating the prime candidate N, according to according to $N = 2 \times$ (the multiplication value $R + w$) $\times$ the prime $q + 1$, using w

satisfying $2 \times w \times$ the prime $q + 1$ = the verification value (*mod* the management information);

a primality testing step of testing primality of the calculated prime candidate N; ~~and~~

an output step of outputting the calculated prime candidate N as [[a]] the prime N when the primality of the calculated prime candidate N is determined; and

a key output step of outputting the private key and the public key of an RSA encryption system to the terminal, the private key and the public key being generated using the prime N output by the output step.

Claim 31 (Cancelled)

Claim 32 (Cancelled)

Claim 33 (Currently Amended) A prime verification method used in a key verification server ~~prime verification~~ apparatus that (i) verifies ~~the~~ a prime N output from a key issuing server ~~prime calculating~~ apparatus for calculating a prime candidate N larger than a known prime q, testing primality of the calculated prime candidate N, and generating and issuing a public key and a private key of an RSA encryption system for a terminal, the key issuing server apparatus including an information storage unit storing the known prime q, management information that is an odd number and corresponds to a prime to be generated, and a predetermined verification value, a random number generation unit operable to generate a random number, a candidate calculation unit operable to (a) read the prime q, the management information, and the verification value, (b) calculate a multiplication value R by multiplying the management

information by the random number, and (c) calculate the prime candidate N, according to $N = 2 \times$ (the multiplication value $R + w$) $\times$ the prime $q + 1$, using w satisfying $2 \times w \times$ the prime $q + 1 =$ the verification value (*mod* the management information), a primality testing unit operable to test primality of the calculated prime candidate N, an output unit operable to output the calculated prime candidate N as the prime N when the primality of the calculated prime candidate N is determined, and a key output unit operable to output the private key and the public key of the RSA encryption system to the terminal, the private key and the public key being generated using the prime N output by the output unit ~~of Claim 1~~, and (ii) includes an information storage unit storing the management information and the verification value, the prime verification method comprising:

a subtraction step of obtaining a prime subtraction value by subtracting the verification from the prime N;

a judgment step of judging whether the obtained prime subtraction value is divisible by the management information; and

a control step of permitting use of the prime N when the judgment by the judgment step is affirmative, and prohibiting the use of the prime N when the judgment by the judgment step is negative.

Claim 34 (Currently Amended) A computer-readable recording medium having a prime-verification computer program recorded thereon, the prime-verification computer program being used on a key verification server apparatus ~~prime verification apparatus~~ that (i) verifies ~~the~~ a prime N output from a key issuing server apparatus ~~prime calculating apparatus~~ for calculating a

prime candidate N larger than a known prime q, testing primality of the calculated prime candidate N, and generating and issuing a public key and a private key of an RSA encryption system for a terminal, the key issuing server apparatus including an information storage unit storing the known prime q, management information that is an odd number and corresponds to a prime to be generated, and a predetermined verification value, a random number generation unit operable to generate a random number, a candidate calculation unit operable to (a) read the prime q, the management information, and the verification value, (b) calculate a multiplication value R by multiplying the management information by the random number, and (c) calculate the prime candidate N, according to $N = 2 \times$ (the multiplication value $R + w$) $\times$ the prime $q + 1$, using w satisfying $2 \times w \times$ the prime $q + 1$ = the verification value (*mod* the management information), a primality testing unit operable to test primality of the calculated prime candidate N, an output unit operable to output the calculated prime candidate N as a prime N when the primality of the calculated prime candidate N is determined, and a key output unit operable to output the private key and the public key of the RSA encryption system to the terminal, the private key and the public key being generated using the prime N output by the output unit ~~of Claim 1~~, and (ii) includes an information storage unit storing the management information and the verification value, the prime-verification computer program causing the key verification server apparatus to execute a ~~prime verification~~ method comprising:

a subtraction step of obtaining a prime subtraction value by subtracting the verification from the prime N;

a judgment step of judging whether the obtained prime subtraction value is divisible by the management information; and

a control step of permitting use of the prime *N* when the judgment by the judgment step is affirmative, and prohibiting the use of the prime *N* when the judgment by the judgment step is negative.

Claim 35 (Cancelled)

Claim 36 (Cancelled)